

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-109439
 (43)Date of publication of application : 12.04.2002

(51)Int.Cl. G06F 17/60
 B42D 15/10
 G06F 15/00
 G06K 17/00
 G06K 19/077
 G06K 19/07

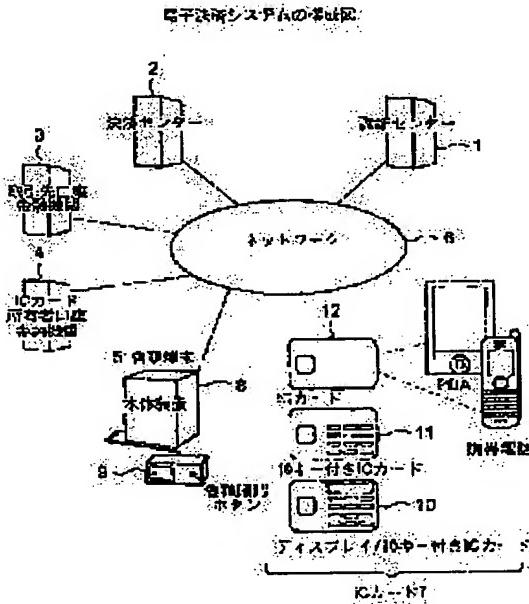
(21)Application number : 2000-301281 (71)Applicant : RICOH CO LTD
 (22)Date of filing : 29.09.2000 (72)Inventor : YANO TAKASHI

(54) ELECTRONIC ACCOUNT SETTLEMENT SYSTEM, IC CARD, ELECTRONIC SETTLEMENT EQUIPMENT AND RECORDING MEDIUM IN WHICH THE PROGRAM IS RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic account settlement system which improves the security by preventing an illegal recording of a password or information on a living body and also by preventing an illegal settlement.

SOLUTION: This system is an electronic account settlement system which performs an electronic settlement using an IC card, that is, it performs a transaction of an electronic settlement using personal information which is input in the IC card by a user beforehand and information about transaction amount, etc. The personal information consists of a password and the information on a living body, and by which a personal certification is performed. The information about transaction amount, etc., consists of a maximum transaction amount limit and a transaction amount, and the transaction by a false transaction amount is prevented by transmitting from the IC card the maximum transaction amount limit and the transaction amount to the electronic settlement equipment.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-109439

(P2002-109439A)

(43)公開日 平成14年4月12日 (2002.4.12)

(51)Int.Cl. ¹	識別記号	F I	マークコード(参考)
G 06 F 17/60	4 1 4	G 06 F 17/60	4 1 4 2 C 0 0 5
	2 4 2		2 4 2 5 B 0 3 5
	5 1 0		5 1 0 5 B 0 4 9
B 42 D 15/10	5 2 1	B 42 D 15/10	5 2 1 5 B 0 5 5
G 06 F 15/00	3 3 0	G 06 F 15/00	3 3 0 G 5 B 0 5 8

審査請求 未請求 請求項の数25 O L (全 13 頁) 最終頁に続く

(21)出願番号 特願2000-301281(P2000-301281)

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(22)出願日 平成12年9月29日 (2000.9.29)

(72)発明者 矢野 隆志

東京都大田区中馬込1丁目3番6号 株式
会社リコー内

(74)代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

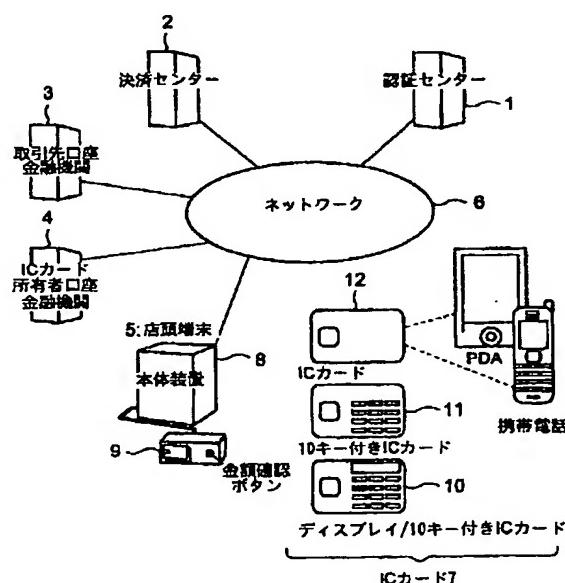
(54)【発明の名称】電子決済システム、ICカード、決済装置、及びそのプログラムを記録した記録媒体

(57)【要約】

【課題】パスワードや生体情報の不正な記録を防止し、不正な決済を防止することによりセキュリティ向上させた電子決済システムを提供することを目的とする。

【解決手段】ICカードを用いて電子決済を行う電子決済システムであり、利用者によって予めICカードに入力された個人情報や取引額等の情報を用いて電子決済における処理を行う。個人情報はパスワードや生体情報であり、これにより個人認証を行う。取引額等の情報は取引限度額や取引額であり、ICカードから取引限度額や取引額を決済装置に送信することにより、不正な取引による取引が行われることを防止する。

電子決済システムの構成図



【特許請求の範囲】

【請求項 1】 ICカードを用いて電子決済を行う電子決済システムであって、利用者によって予めICカードに入力された情報を用いて電子決済における処理を行うことを特徴とする電子決済システム。

【請求項 2】 前記情報は個人情報であり、該個人情報を用いてICカードの認証処理を行う請求項1に記載の電子決済システム。

【請求項 3】 前記電子決済システムは認証装置を有し、前記認証処理において、

前記ICカードは属性情報を認証装置に送信し、該認証装置は認証信号を該ICカードに送信し、該ICカードは該認証信号と前記個人情報を含む情報を演算を施し、認証応答信号を生成して該認証装置に送信し、

該認証装置が該認証応答信号を用いて認証を行う請求項2に記載の電子決済システム。

【請求項 4】 前記ICカードに入力された個人情報を一回の取引における使用に限定する請求項2又は3に記載の電子決済システム。

【請求項 5】 前記個人情報はパスワード又は生体情報である請求項2ないし4のうちいずれか1項に記載の電子決済システム。

【請求項 6】 前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する請求項1に記載の電子決済システム。

【請求項 7】 前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引限度額であり、

前記ICカードは取引限度額を決済装置に送信し、決済装置は、該取引限度額を受信し、店頭端末からICカードの利用者の取引額を含む取引要求を受信し、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する請求項6に記載の電子決済システム。

【請求項 8】 前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引額であり、

前記ICカードは取引額を決済装置に送信し、決済装置は、該取引額を受信し、前記店頭端末からICカードの利用者の取引額を含む取引要求を受信し、ICカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する請求項6に記載の電子決済システム。

【請求項 9】 前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引限度額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたICカードに、該店頭端末から取引限度額を超える取引要求がある場合に該ICカードは該取引要求を拒絶する請求項6に記載の電子決済シ

ステム。

【請求項 10】 前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたICカードに、前記店頭端末から前記取引額と異なる取引額による取引要求がある場合に該ICカードは該取引要求を拒絶する請求項6に記載の電子決済システム。

【請求項 11】 店頭端末を有する電子決済システムで使用するICカードであって、

テンキーと、
テンキーを用いて入力された情報を保持する手段と、
該情報を店頭端末に送信する手段とを有することを特徴とするICカード。

【請求項 12】 テンキーを用いて入力された情報を表示するディスプレイを更に有する請求項11に記載のICカード。

【請求項 13】 入力された情報を所定の処理の後に削除する手段を更に有する請求項11に記載のICカード。

【請求項 14】 消費税を算出するためのキーを更に有する請求項12又は13に記載のICカード。

【請求項 15】 前記電子決済システムが電子マネー型である場合において、
前記情報として取引限度額を保持する手段と、
店頭端末から取引限度額を超える取引要求がある場合に該取引要求を拒絶する手段とを更に有する請求項11に記載のICカード。

【請求項 16】 前記電子決済システムが電子マネー型である場合において、
前記情報として取引額を保持する手段と、
店頭端末から前記取引額と異なる取引額による取引要求がある場合に該取引要求を拒絶する手段とを更に有する請求項11に記載のICカード。

【請求項 17】 ICカードを用いて電子決済を行う電子決済システムにおける決済装置であって、
利用者によって予めICカードに入力された情報を受信し、その情報を用いて電子決済における処理を行うことを特徴とする決済装置。

【請求項 18】 前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手段を有する請求項17に記載の決済装置。

【請求項 19】 前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、前記ICカードから取引限度額を受信する手段と、
店頭端末からICカードの利用者の取引額を含む取引要求を受信する手段と、
該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手段とを有する請求項18に記載の決済装置。

【請求項 2 0】 前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、前記 I C カードから取引額を受信する手段と、店頭端末から I C カードの利用者の取引額を含む取引要求を受信する手段と、I C カードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手段とを有する請求項 1 8 に記載の決済装置。

【請求項 2 1】 I C カードを用いて電子決済を行う電子決済システムにおける決済処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

利用者によって予め I C カードに入力された情報を受信し、その情報を用いて電子決済における処理手順をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 2】 前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手順を有する請求項 2 1 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 3】 前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、前記 I C カードから取引限度額を受信する手順と、店頭端末から I C カードの利用者の取引額を含む取引要求を受信する手順と、

該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手順とを有する請求項 2 2 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 4】 前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、前記 I C カードから取引額を受信する手順と、店頭端末から I C カードの利用者の取引額を含む取引要求を受信する手順と、

I C カードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手順とを有する請求項 2 2 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 5】 I C カードを用いて電子決済を行う電子決済システムであって、I C カードに所定の情報を入力する第 1 の端末と、前記 I C カードから所定の情報を取り出して操作部から入力された取引の情報に関する情報とともに送信する第 2 の端末とを有する電子決済システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】 本発明は、商取引によって発生する購入代金、使用料等の決済をネットワークや I C カードを利用して行う電子決済に関する。

【0 0 0 2】

【従来の技術】 電子決済にはネットワーク型電子決済とカード型電子決済がある。ネットワーク型電子決済は仮想世界の商取引に使用され、電子財布と呼ばれる概念のソフトウェアで貨幣価値の保存、転送を行う。カード型電子決済は実世界の商取引に使用することができ、メモリーで貨幣価値の保存を行う。本発明はこれらのうちのカード型電子決済、特に I C カードを利用したカード型電子決済を対象としており、以下、カード型電子決済の従来技術について説明する。

【0 0 0 3】 カード型電子決済には、クレジットカード型、電子マネー型、キャッシュカード型の 3 種類の方式がある。

【0 0 0 4】 クレジットカード型におけるカードはクレジット会社が発行し、決済は 25~55 日後に所有者の銀行口座から引き落とされ、取引先の銀行口座に振り込まれることにより行われる。クレジットカード型では本人認証にサインを用いるので支払に手間がかかり、使用は一般的に高額の取引に限定される。

【0 0 0 5】 電子マネー型には例えビザ・キャッシュ、モンデックス、プロトン、スーパーキャッシュ等があり、電子マネーは主に金融機関が発行する。電子マネー型で使用するカードが記憶しているのは貨幣価値情報であり、カードを使用する際には本人確認の必要はなく、他人の使用もできる。決済は貨幣価値情報の転送でリアルタイムに行われ、主に少額取引に用いられる。

【0 0 0 6】 電子マネー型では、店頭端末における目視による金額確認と確認ボタンの操作(決済がその場で完結し証拠が残らないため)が必要であること等のため、あまり普及していない。

【0 0 0 7】 キャッシュカード型には例えビットカードがあり、カードは主に金融機関が発行する。本人確認は所有者のパスワード(例え銀行口座暗証番号)で行われ、決済はリアルタイムに所有者の銀行口座から引き落とされ取引先の銀行口座に振り込まれる。預金残高以上の取引はできず、主に少額取引に用いられる。

【0 0 0 8】 キャッシュカード型における本人確認には所有者のパスワード(銀行口座暗証番号)が用いられ、これが盗まれると所有者の銀行口座の預金が危険にさらされるとする問題点がある。

【0 0 0 9】 さて、上記の電子決済システムには利用者が用いるカードとして磁気カード等や I C カードが用いられる。磁気カード等を用いた場合にはユーザ認証をユーザ ID (カード ID) とパスワード(ユーザが入力するパスワード)によって行っており、ユーザ ID とパスワードが容易に傍受されるという問題がある。一方、I C カードは磁気カード等と比較して情報の読みだしが困難であり、偽造も困難である。また、暗号処理を行うことにより、パスワードによるユーザ認証を暗号アルゴリズムを用いて行い、更に、耐タンパー性を持たせる(漏洩

電磁波のシールド等)ことにより、磁気カード等と比較してユーザ認証能力と偽造防止能力が高い。

【0010】

【発明が解決しようとする課題】しかしながら、ICカードを用いた電子決済システムでも、利用者はICカードの所有者であることを証明するために店頭端末にパスワードを入力することが必要である。この時、パスワードを第三者に見られる可能性があり、また、店頭端末に直接パスワードを入力するために悪意によって改造された店頭端末によってパスワードの記録を取られる可能性がある。従って、パスワードが盗まれる可能性があるという問題点がある。パスワードが盗まれると不正な架空の決済が行われる可能性がある。

【0011】指紋等の生体情報の認識技術であるバイオメトリックスもユーザ認証に使用されてきているが、この場合にも、ICカードの所有者であることの証明に店頭端末で生体情報を読み取る必要があり、悪意によって改造された店頭端末によって生体情報を記録される可能性がある。

【0012】また、上記従来の技術によると、ICカード所有者に提供する情報と異なる情報を決済センターに提供することにより不正な決済(異なる金額の決済)が行われる可能性があるという問題点がある。これはパスワードや生体情報が盗まれなくても起こりうる。

【0013】更に、店頭端末へのパスワード入力に時間がかかり、営業効率に影響を及ぼすという問題がある。また、クレジットカード型ではサインの処理に時間を要し、電子マネー型では店頭端末へのパスワード入力、金額確認ボタンの操作に時間を要し、キャッシュカード型では金額確認ボタンの操作に時間を要するという問題点がある。

【0014】本発明は上記の点に鑑みてなされたものであり、パスワードや生体情報の不正な記録を防止し、不正な決済を防止することによりセキュリティを向上させ、更に店頭端末における操作時間を短縮させた電子決済システムを提供することを目的とする。

【0015】

【課題を解決するための手段】上記の目的を達成するために本発明は次のように構成することができる。

【0016】請求項1に記載の発明は、ICカードを用いて電子決済を行う電子決済システムであって、利用者によって予めICカードに入力された情報を用いて電子決済における処理を行う。

【0017】本発明によれば、予めICカードに入力された情報を用いるので、改造された店頭端末等により入力情報が記録されるという問題点を解消でき、セキュリティを向上させることができる。また、改造された店頭端末等の不正により実際と異なる取引額による決済が行われることを防止することが可能となる。

【0018】請求項2に記載の発明は、請求項1の記載

において、前記情報は個人情報であり、該個人情報を用いてICカードの認証処理を行うようとする。

【0019】本発明によれば、特に、パスワード等の個人情報が改造された店頭端末等により記録されるという問題点を解消できる。

【0020】請求項3に記載の発明は、請求項2の記載において、前記電子決済システムは認証装置を有し、前記認証処理において、前記ICカードは属性情報を認証装置に送信し、該認証装置は認証信号を該ICカードに送信し、該ICカードは該認証信号と前記個人情報を含む情報に演算を施し、認証応答信号を生成して該認証装置に送信し、該認証装置が該認証応答信号を用いて認証を行う。これにより、ICカード利用者の認証を、個人情報が傍受されることなく行うことができる。

【0021】請求項4に記載の発明は、請求項2又は3の記載において、前記ICカードに入力された個人情報を一回の取引における使用に限定する。

【0022】本発明により、個人情報が盗まれる危険を防止することができる。

【0023】請求項5に記載の発明は、請求項2ないし4のうちいずれか1項の記載において、前記個人情報はパスワード又は生体情報であるとする。パスワード又は生体情報を用いることにより、個人認証を行うことができる。

【0024】請求項6に記載の発明は、請求項1の記載において、前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する。

【0025】本発明によれば、改造された店頭端末等を用いた不正により実際と異なる取引額による決済が行われることを防止することが可能となる。

【0026】請求項7に記載の発明は、請求項6の記載において、前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引限度額であり、前記ICカードは取引限度額を決済装置に送信し、決済装置は、該取引限度額を受信し、店頭端末からICカードの利用者の取引額を含む取引要求を受信し、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する。

【0027】本発明によれば、取引額が取引限度額を超えることがなくなり、不正や過誤により過大な取引額による決済が行われることを防止できる。

【0028】請求項8に記載の発明は、請求項6の記載において、前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引額であり、前記ICカードは取引額を決済装置に送信し、決済装置は、該取引額を受信し、前記店頭端末からICカードの利用者の取引額を含む取引要求を受信し、ICカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒

絶する。

【0029】本発明によれば、不正により実際と異なる取引額による取引要求がなされた場合でも、その取引要求は拒絶されるため、取引の安全を確保でき、セキュリティを高めることができる。また、店頭端末における金額確認が不要となるため、操作が容易になり、利用者の利便性が向上するとともに、店における業務効率も向上する。

【0030】請求項9に記載の発明は、請求項6の記載において、前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引限度額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたICカードに、該店頭端末から取引限度額を超える取引要求がある場合に該ICカードは該取引要求を拒絶する。

【0031】本発明によれば、請求項7と同様の作用効果を得ることができる。

【0032】請求項10に記載の発明は、請求項6の記載において、前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたICカードに、前記店頭端末から前記取引額と異なる取引額による取引要求がある場合に該ICカードは該取引要求を拒絶する。

【0033】本発明によれば、請求項8と同様の作用効果を得ることができる。

【0034】請求項11に記載の発明は、店頭端末を有する電子決済システムで使用するICカードであって、テンキーと、テンキーを用いて入力された情報を保持する手段と、該情報を店頭端末に送信する手段とを有する。

【0035】本発明によれ、上記電子決済システムでの使用に適したICカードを提供することができる。

【0036】請求項12に記載の発明は、請求項11の記載において、テンキーを用いて入力された情報を表示するディスプレイを更に有する。これにより入力を確認することができる。

【0037】請求項13に記載の発明は、請求項11の記載において、入力された情報を所定の処理の後に削除する手段を更に有する。本発明によれば、処理の度に新たに情報を入力することとなるので、セキュリティを高めることができる。

【0038】請求項14に記載の発明は、請求項12又は13の記載において、消費税を算出するためのキーを更に有する。これにより、正確かつ迅速に取引額を入力することができる。

【0039】請求項15に記載の発明は、請求項11の記載において、前記電子決済システムが電子マネー型である場合において、前記情報として取引限度額を保持する手段と、店頭端末から取引限度額を超える取引要求が

ある場合に該取引要求を拒絶する手段とを更に有する。本発明によれば、請求項9の電子決済システムでの使用に適したICカードを提供できる。

【0040】請求項16に記載の発明は、請求項11の記載において、前記電子決済システムが電子マネー型である場合において、前記情報として取引額を保持する手段と、店頭端末から前記取引額と異なる取引額による取引要求がある場合に該取引要求を拒絶する手段とを更に有する。本発明によれば、請求項10の電子決済システムでの使用に適したICカードを提供できる。

【0041】請求項17に記載の発明は、ICカードを用いて電子決済を行う電子決済システムにおける決済装置であって、利用者によって予めICカードに入力された情報を受信し、その情報を用いて電子決済における処理を行う。

【0042】本発明によれば、請求項1と実質的に同様の作用効果を奏する。

【0043】請求項18に記載の発明は、請求項17の記載において、前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手段を有する。

【0044】本発明によれば、請求項6と実質的に同様の作用効果を奏する。

【0045】請求項19に記載の発明は、請求項18の記載において、前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、前記ICカードから取引限度額を受信する手段と、店頭端末からICカードの利用者の取引額を含む取引要求を受信する手段と、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手段とを有する。

【0046】本発明によれば、請求項7と実質的に同様の作用効果を奏する。

【0047】請求項20に記載の発明は、請求項18の記載において、前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、前記ICカードから取引額を受信する手段と、店頭端末からICカードの利用者の取引額を含む取引要求を受信する手段と、ICカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手段とを有する。

【0048】本発明によれば、請求項8と実質的に同様の作用効果を奏する。

【0049】請求項21～請求項24に記載の発明によれば、請求項17～20の決済装置の処理を行うことに適したプログラムを記録した記録媒体を提供することができる。

【0050】また、請求項25に記載の発明は、ICカードを用いて電子決済を行う電子決済システムであつて、ICカードに所定の情報を入力する第1の端末と、前記ICカードから所定の情報を取り出して操作部から

入力された取引の情報に関する情報とともに送信する第2の端末とを有する。

【0051】本発明によれば、請求項1に記載の発明と実質的に同様の作用効果を奏する。

【0052】

【発明の実施の形態】【第1の実施例】図1に本発明の実施例における電子決済システムの構成を示す。同図に示すように、本電子決済システムは、認証センター1(認証装置ともいいう)、決済センター2(決済装置ともいいう)、取引先口座金融機関3、ICカード所有者口座金融機関4、店頭端末5を有し、それぞれがネットワーク6に接続される。また、ICカード7は、店頭端末5に装着されることによりネットワーク6を介してデータを送受信できる。

【0053】認証センター1はICカードの認証を行い、決済センター2が決済処理を行う。取引先口座金融機関3は、取引相手の口座を持つ金融機関であり、ある物を購入した場合の代金はこの口座に振り込まれる。ICカード所有者口座金融機関4は、ICカード所有者の口座を持つ金融機関であり、購入代金がここから引き落としされる。

【0054】認証センター1と決済センター2は、クレジットカード型ではクレジット会社にある。

【0055】また、一般的な電子マネー型ではパスワード認証を行ないので認証センター1はないが、パスワード認証を行う電子マネー型では認証センターが必要であり、本実施例においてはパスワード認証を行うものとして説明する。電子マネー型における決済センター2は銀行等のカード発行金融機関にあり、ICカード所有者はカード発行金融機関に口座を作る。

【0056】キャッシュカード型では認証センター1と決済センター2共に銀行等のカード発行金融機関にあり、この場合もICカード所有者はカード発行金融機関に口座を作る。

【0057】認証センター1と決済センター2はそれぞれコンピュータを用いて実現することができる。図2に決済センター2の構成例を示す。なお、認証センター1も図2に示す構成と同様の構成をとることができる。図2に示すように、決済センター2は、CPU(中央処理装置)101、メモリ102、入力装置103、表示装置104、CD-ROMドライブ105、ハードディスク106、通信処理装置107を有する。CPU101は装置の全体を制御する。メモリ102はCPU101で処理するデータやプログラムを保持する。入力装置103はキーボードやマウス等のデータを入力するための装置である。表示装置104はディスプレイ等の装置である。CD-ROMドライブ105はCD-ROM等を駆動し、データやプログラムの読み出しが行う。ハードディスク106には、プログラムや、本発明の処理に関わるデータが格納される。通信処理装置107によりデ

ータをネットワークを介して送受信する。また、データの保存等ためにMT装置を接続してもよい。本発明の電子決済処理を実行するプログラムは、コンピュータに予めインストールされていてもよいし、例えばCD-ROMに格納され、CD-ROMドライブ105を介してハードディスク106にロードするようにしてもよい。プログラムが起動されると、所定のプログラム部分がメモリ102に展開され、処理が実行される。

【0058】なお、認証センター1と決済センター2を統合することも可能である。また、認証センター1と決済センター2をカード発行金融機関から独立させ、電子マネー/キャッシュカードの運営グループの運営とすることもできる。

【0059】取引先口座金融機関3、ICカード所有者口座金融機関4の構成及び動作は従来と同様である。

【0060】店頭端末5は、本体装置8とICカードを装着するリーダーライター9を有する。本体装置8は例えばコンピュータを用いて実現できる。また、本体装置8をPOS端末としてもよい。また、本体装置とリーダーライターを一体として構成することもできる。

【0061】ネットワーク6としては、例えばインターネット、回線交換ネットワーク、専用回線を使用することができる。

【0062】図1に示すように、ICカードとしては、ディスプレイとテンキー付きICカード10、テンキー付きICカード11、PDAや携帯電話とのインターフェースを有するICカード12を使用できる。

【0063】ディスプレイとテンキー付きICカード10の構成を図3に示す。

【0064】ディスプレイとテンキー付きICカード10は、店頭端末等から信号や電力を受信するアンテナ21、信号の送受信を行うトランシーバ22、処理・制御を行うCPU23、入力データ等を保持するRAM24、プログラムと秘密鍵を記憶するE PROM25(一般的にはフラッシュメモリーが用いられる)、情報を入力するためのテンキー26、テンキーからの入力を符号化するテンキーエンコーダ27、情報を表示するLCD(liquid crystal display)28、LCDを制御するディスプレイドライバ29、アンテナや電池内蔵ウォレットから受信した電力を受電する受電器30、電力を蓄えるキャパシタ31、受電器30からの電力とキャパシタ31を切替えるための切替器32を有する。

【0065】上記の構成において、LCD28、ディスプレイドライバ29を省略した構成とすることもでき、その場合、アンテナを介してデータを送受信することによりPDAや携帯電話にディスプレイ機能を持たせることが可能である。

【0066】上記のように電源としてキャパシタ31又は二次電池を使用し、充電は接触型/非接触型とともに次のようにして行うことができる。すなわち、電池内蔵

ウォレットに装着した状態で充電しながらキー操作を行い電池内蔵ウォレットからICカードを取り外す。また、電池内蔵ウォレットに装着して充電し、電池内蔵ウォレットからICカードを取り外した状態でキー操作を行うようにしてもよい。また、店頭端末のリーダーライターに装着した時に充電してもよい。

【0067】図4にPDAや携帯電話とのインターフェースを有するICカード12の構成を示す。同図に示すように、図3に示す構成からテンキーとLCDに関わる部分を除いた構成となる。この場合、EPROM25には、プログラムと秘密鍵と共に、携帯電話やPDAの認証に用いる公開鍵を有する。また、PDAや携帯電話から操作時に電力を供給することが可能である。

【0068】次に、本発明の第1の実施例における処理手順を図5を用いて説明する。

【0069】まず、ICカード所有者はテンキー付きICカード、ディスプレイ/テンキー付きICカード、又はPDA、携帯電話等を用いて、ICカードにパスワードを入力する（ステップ1）。パスワードの表示は“*”等の記号を用いるか、“Enter”キー入力で消去される（ディスプレイなしのICカードではこの制御は不要である。）。なお、パスワードや生体情報等の個人を証明するための情報を本明細書では個人情報という。

【0070】次に、利用者はICカードを店頭端末のリーダーライターに装着する（ステップ2）。なお、非接触型ICカードを用いる場合は接近させるだけでよい。

【0071】続いて、ICカードは属性情報を認証センターに送る（ステップ3）。属性情報を受信した認証センターは認証信号をICカードに送る（ステップ4）。この認証信号は認証の度に異なる値となる。認証信号を受信したICカードは一回のパスワード入力に対して一回のみ、認証信号とパスワードとを連結したデータに例えば秘密鍵による暗号化を施して認証応答信号を生成し、認証センターに送り返す（ステップ5）。上記の属性情報は例えばカードIDである。

【0072】認証センターは認証応答信号を公開鍵で復号化し、認証センターが有する当該ICカードの属性情報に対するパスワードと、復号化して得たパスワードとを比較して正しいことを確認すると、認証済信号を店頭端末に送り（ステップ6）、認証応答信号が正しくないことを確認すると認証拒否信号を店頭端末に送る（ステップ7）。

【0073】上記の例の認証処理の場合、認証センターは図6に示すようなテーブルを有し、このテーブルに記録されたパスワードと、演算によって得たパスワードとの比較を行うことによってパスワード認証を行う。

【0074】なお、上記のようにパスワードを用いず、認証センターから送信された認証信号を秘密鍵で暗号化して認証センターに送り返し、認証センターがそれを復号することでICカード自体の認証を行うことは可能で

ある。この場合のパスワードは、例えば、ICカードを有効にするために使用できる。

【0075】ICカードが一回のパスワード入力に対して一回のみ認証を行うようにするには、例えば、図7に示す処理を行う。すなわち、パスワードを入力し（ステップ101）、上記の認証処理を行い（ステップ102）、認証処理が終了したらICカード内のパスワードを削除する（ステップ103）。

【0076】上記の説明ではパスワードを例にとって説明したが、指紋等の生体情報やその他の個人情報を認証に使用する場合にも同様に処理を行うことが可能である。

【0077】さて、パスワード認証処理以降の処理は電子決済の方式により異なるので、それについて分けて説明する。

【0078】まず、クレジットカード型決済処理について説明する。

【0079】ICカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ11）。次に、店頭端末は決済センター（クレジット会社）に取引額の支払を要求し（ステップ12）、決済センター（クレジット会社）は決済日に所有者の銀行口座から要求額を引き落とし、取引先（加盟店）の口座に取引額から手数料を減算した金額を振り込む（ステップ13）。

【0080】次に、電子マネー型決済処理について説明する。

【0081】上記と同様に、ICカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ21）。次に、店頭端末はICカードの貨幣価値情報を取引額だけ減算し取引先（加盟店）の貨幣価値情報を加算し（ステップ22）、決済センター（カード発行金融機関）に獲得した貨幣価値情報を送る（ステップ23）。決済センター（カード発行金融機関）は取引先（加盟店）の口座に貨幣価値情報の金額を振り込む（ステップ24）。なお、手数料がある場合はそれを減算した金額を振り込む。

【0082】次に、キャッシュカード型決済処理について説明する。

【0083】ICカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ31）。店頭端末は決済センター（カード発行金融機関）に取引額の支払を要求し（ステップ32）、決済センター（カード発行金融機関）は所有者口座から要求額を引き落とし、取引先（加盟店）の口座にその金額を振り込む（ステップ33）。なお、手数料がある場合はそれを減算した金額を振り込む。

【0084】なお、上記の各決済センターは、各処理の履歴の管理・報告等も行う。

【0085】【第2の実施例】次に、本発明の第2の実施例について、図8を用いて説明する。

【0086】第2の実施例では、パスワードに加え、ICカードに取引限度額を入力する。これにより、取引限度額を超える取引を防止することができ、安全に取引を行うことができる。

【0087】まず、第1の実施例で説明したように、パスワードをICカードに入力する（ステップ41）。次に、ICカードに取引限度額を入力する（ステップ42）。

【0088】統いて、ICカードを店頭端末のリーダライターに装着することによって、第1の実施例で説明したようなパスワード認証処理が行われる（ステップ43）。

【0089】これ以降の処理は電子決済の方式により異なるので、それぞれについて分けて説明する。

【0090】まず、クレジットカード型決済処理について説明する。

【0091】ICカードは属性情報と取引限度額情報を決済センターに送る（ステップ51）。ICカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ52）。なお、この処理は省略してもよい。そして、店頭端末は決済センター（クレジット会社）に取引額の支払を要求する（ステップ53）。決済センター（クレジット会社）はICカードの取引限度額を越えた取引先（加盟店）からの取引要求を拒絶する（ステップ54）。取引限度額を超えていない場合には、決済センター（クレジット会社）は決済日に所有者の銀行口座から要求額を引き落とし、取引先（加盟店）の口座に取引額から手数料を減算した金額を振り込む（ステップ55）。

【0092】図9に、上記の決済センターの処理フローを示す。まず、取引限度額をICカードから受信する（ステップ111）。その後、取引額を店頭端末から受信する（ステップ112）。そして、取引額と取引限度額とを比較し（ステップ113）、取引額が取引限度額以上であれば取引要求を拒絶し（ステップ114）、取引額が取引限度額より小さければ上述した口座処理を行う（ステップ115）。

【0093】次に、電子マネー型決済処理について説明する。

【0094】ICカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ61）。なお、この処理は省略してもよい。次に、ICカードは、店頭端末からICカードの取引限度額を越える決済要求があるとき、その決済要求を拒絶する（ステップ62）。

【0095】店頭端末からの決済要求がICカードの取引限度額を超えない場合には、店頭端末はICカードの貨幣価値情報を取引額だけ減算し取引先（加盟店）の貨幣価値情報を加算する（ステップ63）。統いて、店頭端末は決済センター（カード発行金融機関）に獲得した貨幣

価値情報を送る（ステップ64）。

【0096】決済センター（カード発行金融機関）は取引先（加盟店）の口座に貨幣価値情報の金額を振り込む（ステップ65）。なお、手数料がある場合はそれを減算した金額を振り込む。

【0097】上記の電子マネー型の場合の取引限度額判断に係わるICカードの処理フローを図10に示す。まず、店頭端末から決済要求とともに取引額を受信する（ステップ121）。その取引額とユーザが入力した取引限度額とを比較し（ステップ122）、取引額が取引限度額以上であれば決済要求を拒絶し（ステップ123）、取引額が取引限度額より小さければICカードの貨幣価値情報を取引額だけ減算する（ステップ124）。

【0098】次に、キャッシュカード型決済処理について説明する。

【0099】まず、ICカードは属性情報と取引限度額情報を決済センターに送る（ステップ71）。統いて、ICカード所有者（ユーザ）は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ72）。なお、この処理は省略することが可能である。次に、店頭端末は決済センター（カード発行金融機関）に取引額の支払を要求する（ステップ73）。要求を受けた決済センター（カード発行金融機関）はICカードからの取引限度額を越えた取引先（加盟店）からの決済要求を拒絶する（ステップ74）。

【0100】決済要求がICカードからの取引限度額を超えない場合には決済センター（カード発行金融機関）は所有者口座から要求額を引き落とし、取引先（加盟店）の口座に該金額を振り込む（ステップ75）。なお、手数料がある場合はそれを減算した金額を振り込む。この場合の決済センターの処理フローは図9に示した処理フローと同様である。

【0101】第2の実施例において、支払額データをICカードに書き込み、必要に応じて表示することにより、取引限度額までいくらあるかを容易に把握することができる。

【0102】【第3の実施例】次に、第3の実施例を図11を用いて説明する。第3の実施例では、パスワードに加え、ICカードに取引額を入力する。これにより、安全に取引を行うことができるとともに、金額確認の操作を省略することが可能である。以下、第1、第2の実施例と異なる部分を中心に説明する。

【0103】利用者は、店頭端末にICカードを装着する前にICカードに取引額を入力する（ステップ81）。ここで、第3の実施例で使用するICカードには、正確な取引額を入力するために消費税を加算するキーを設けるようにしてもよい。このキーには、ディスプレイ/テンキー付きICカードを使用する方式ではボタンを使用し、PDAや携帯電話で情報をICカードに入

力する方式ではボタンでもソフトスイッチでも使用可能である。このようなキーを用いて、購入した複数商品の総額や消費税の加算の計算を行い、ICカードに正確な取引額を入力する。この後、ICカードを店頭端末に装着し（ステップ82）、パスワード認証（ステップ83）が行われる。

【0104】クレジットカード型、キャッシュカード型の場合、パスワード認証の後にICカードは属性情報と取引額情報を決済センターに送る（ステップ84）。そして、店頭端末は決済センターに取引額の支払を要求する（ステップ85）。なお、第3の実施例では取引額を利用者がICカードに入力しているため、店頭端末による金額確認は行わない。

【0105】決済センターは、ICカードから受信した取引額と異なる取引額の支払いを要求した取引先からの取引要求を拒絶する（ステップ86）。ICカードから受信した取引額と店頭端末からの取引額が一致した場合には、第1、2の実施例で説明した引き落とし、振り込み処理等の口座処理が行われる。

【0106】電子マネー型の場合、ICカードは、ICカードに入力された取引額と異なる決済要求が店頭端末からあるとき、その決済要求を拒絶する（ステップ91）。店頭端末からの決済要求がICカードの取引額と一致する場合には、第2の実施例で説明した電子マネー型決済処理におけるステップ63以降と同様の決済処理が行われる。

【0107】上記の決済センターの処理フローを図12に示す。まず、ICカードから予め入力された取引額を受信する（ステップ131）。次に、店頭端末から取引要求とともに取引額を受信する（ステップ132）。これらの取引額を比較し（ステップ133）、一致しなければ取引要求を拒絶し（ステップ134）、一致する場合には口座処理を行う（ステップ135）。

【0108】次に、電子マネー型の場合の取引限度額判断に係わるICカードの処理フローを図13に示す。まず、店頭端末から決済要求とともに取引額を受信する（ステップ141）。その取引額とユーザが入力した取引額とを比較し（ステップ142）、それらが一致しなければ決済要求を拒絶し（ステップ143）、一致すればICカードの貨幣価値情報を取引額だけ減算する（ステップ144）。

【0109】なお、第2と第3の実施例を組み合わせて、取引限度額と取引額をICカードに入力するようにしてもよい。

【0110】本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【0111】

【発明の効果】本発明によれば、店頭端末にICカードを装着する前にパスワードを入力するので、店頭端末の

改造等によってパスワードを記録される危険を無くすことができる。また、店頭端末へのパスワード入力時間を削減し、利用者の利便性が向上するとともに、店における業務効率を向上させることができる。

【0112】パスワードに係るセキュリティーが向上することにより、クレジットカード型では、本人認証をサインからパスワードに代えることでき、事務経費の削減により手数料を低額にできるという効果がある。また、電子マネー型では、ICカードの収納額を高額にすることができます。更に、キャッシュカード型では、パスワード（銀行口座暗証番号）が盗まれることの問題を解決できる。

【0113】また、取引限度額をICカードに入力し、それを決済センターに送信等することとしたので、店頭端末の改造等による不正や本人の過誤による過大な額の取引を防止することが可能となる。

【0114】また、消費税を含めた取引額をICカードに入力し、その額と店頭端末が算出した取引額とを比較し、一致した場合にのみ取引を行うこととしたため、店頭端末の改造等による不正な取引を防止することが可能となる。また、店頭端末への金額確認ボタンの操作が不要になるため、利用者の利便性が向上するとともに、店における業務効率を向上させることができる。特に、電子マネー型では小額取引が多いので、金額確認ボタン操作不要の効果は大きい。

【0115】上記のようにセキュアで利便性の高い電子決済システムを提供することが可能になるので、当該電子決済システムの運営者はより多くのクライアントと加盟店を確保でき、より多くの取引に利用されることを期待することができる。

【0116】

【図面の簡単な説明】

【図1】電子決済システムの構成図である。

【図2】決済センターの構成図である。

【図3】ディスプレイとテンキー付きICカードの構成図である。

【図4】PDA等とのインターフェースを有するICカードの構成図である。

【図5】本発明の第1の実施例における処理手順を示す図である。

【図6】認証センターが有するテーブルの例を示す図である。

【図7】ICカードが一回のパスワード入力に対して一回のみ認証を行うようにするための処理を示すフローチャートである。

【図8】本発明の第2の実施例における処理手順を示す図である。

【図9】本発明の第2の実施例における決済センターの処理を示すフローチャートである。

【図10】本発明の第2の実施例における電子マネー型

の場合の ICカードの処理を示すフローチャートである。

【図1 1】本発明の第3の実施例における処理手順を示す図である。

【図1 2】本発明の第3の実施例における決済センターの処理を示すフローチャートである。

【図1 3】本発明の第3の実施例における電子マネー型の場合の ICカードの処理を示すフローチャートである。

【符号の説明】

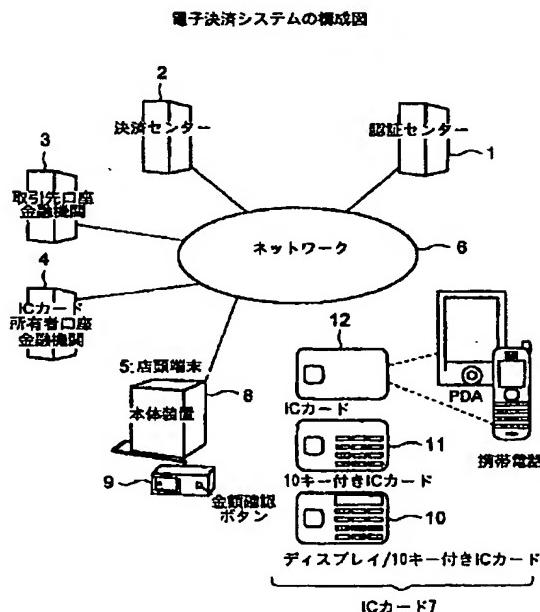
- 1 認証センター
- 2 決済センター
- 3 取引先口座金融機関
- 4 ICカード所有者口座金融機関
- 5 店頭端末
- 6 ネットワーク
- 7 ICカード
- 8 本体装置
- 9 リーダーライター
- 10 ディスプレイとテンキー付き ICカード
- 11 テンキー付き ICカード

【図1】

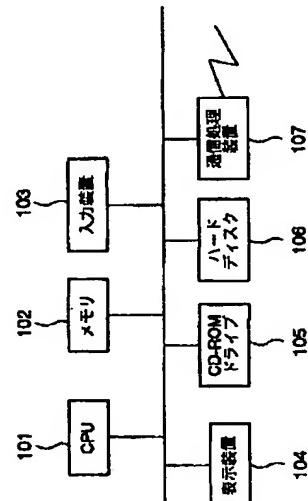
12 PDAや携帯電話とのインターフェースを有する ICカード

- 21 アンテナ
- 22 トランシーバ
- 23 CPU
- 24 RAM
- 25 EPROM
- 26 テンキー
- 27 テンキーエンコーダ
- 28 LCD (liquid crystal display)
- 29 ディスプレイドライバ
- 30 受電器
- 31 キャパシタ
- 32 切替器32
- 101 CPU (中央処理装置)
- 102 メモリ
- 103 入力装置
- 104 表示装置
- 105 CD-ROMドライブ
- 106 ハードディスク
- 107 通信処理装置

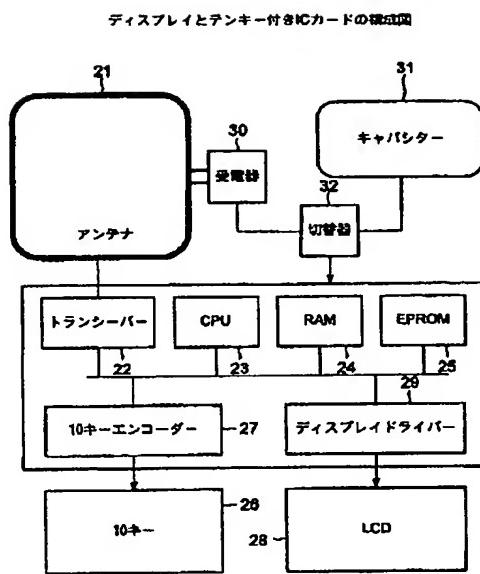
【図2】



決済センターの構成図

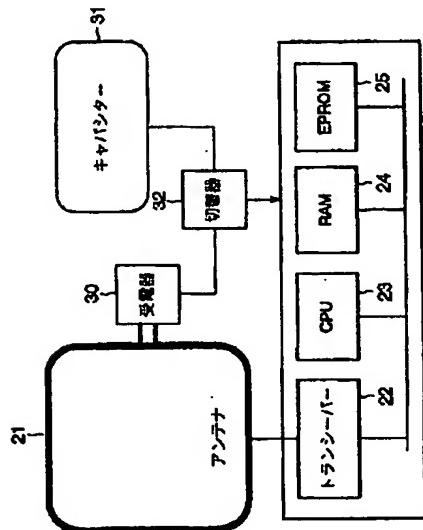


【図3】



【図4】

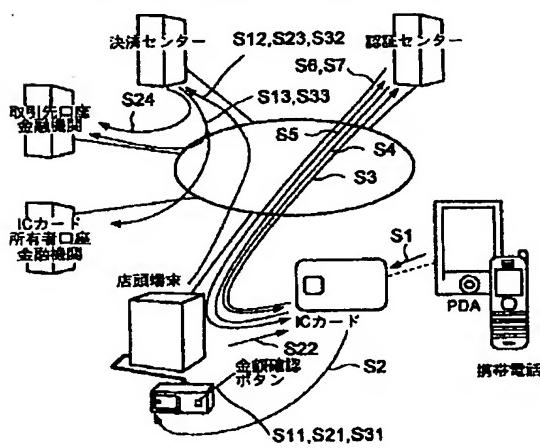
PDA等とのインターフェースを有するICカードの構成図



【図5】

【図6】

本発明の第1の実施例における処理手順を示す図

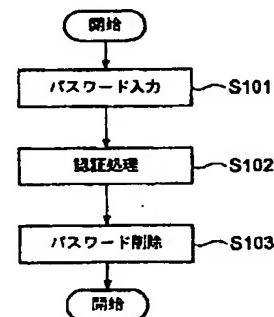


認証センターが有するテーブルの例を示す図

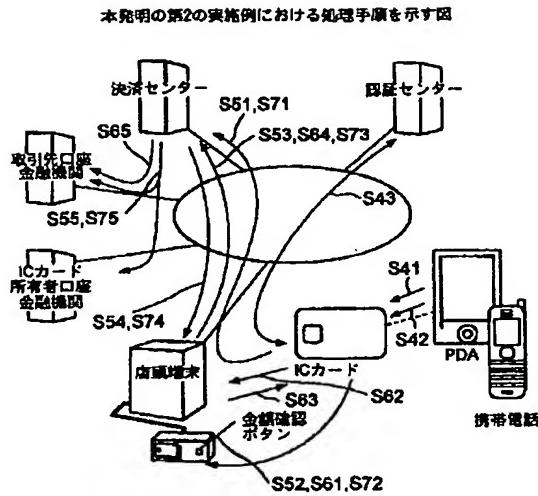
属性情報	パスワード
abcd	× × × ×
efgh	△ △ △ △
⋮	⋮

【図7】

ICカードが一回のパスワード入力に対して一回のみ認証を行いうようにするための処理を示すフローチャート

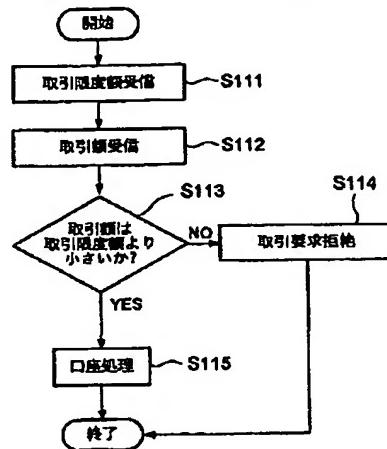


【図 8】



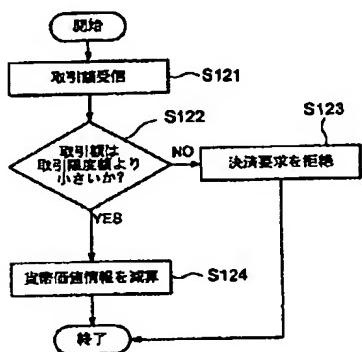
【図 9】

本発明の第2の実施例における決済センターの処理を示すフローチャート



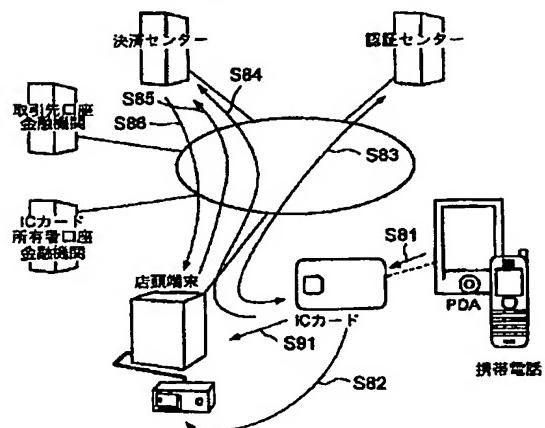
【図 10】

本発明の第2の実施例における電子マネー型の場合のICカードの処理を示すフローチャート



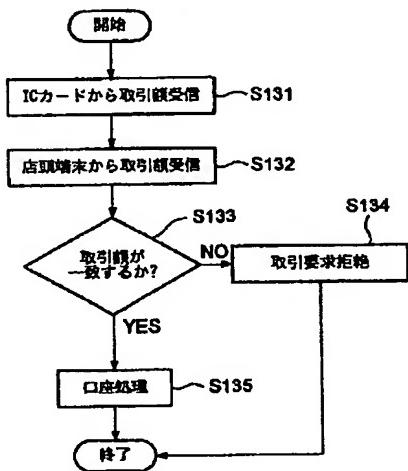
【図 11】

本発明の第2の実施例における処理手順を示す図



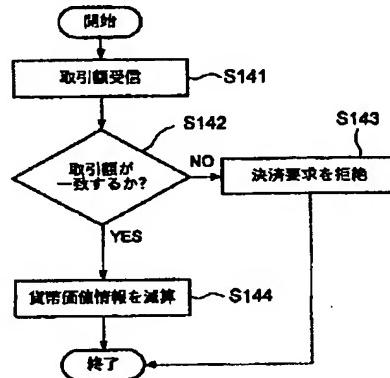
【図12】

本発明の第3の実施例における決済センターの
処理を示すフローチャート



【図13】

本発明の第3の実施例における電子マネー型の場合のICカードの
処理を示すフローチャート



フロントページの続き

(51) Int. Cl. 7 識別記号
 G 0 6 K 17/00
 19/077
 19/07

F I
 G 0 6 K 17/00
 19/00

テーマコード(参考)
 V 5 B 0 8 5
 K
 J

F ターム(参考) 2C005 MA04 MA05 MA33 MB08 NA09
 QA05 QB01 QC20 SA04 SA05
 SA06 SA12 SA13 SA16 TA22
 5B035 AA15 BB09 CA05 CA06
 5B049 AA05 CC39 DD04 EE21 EE26
 5B055 CB00 HA02 KK05 KK19
 5B058 KA38 YA01
 5B085 AA08 AE02 AE12